IN THE CLAIMS

Claims 1 - 6. (Withdrawn)

7. (Currently Amended) A method of securely receiving content data on a user's system from a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:

receiving ~~promotional metadata~~encrypted content data from a ~~first web~~ broadcast channel, wherein the encrypted content data is encrypted with a first encrypting key having a corresponding first decrypting key ~~the promotional metadata related to encrypted content data;~~

~~assembling at least part of the promotional metadata into a promotional offering for review by a user;~~

~~selecting by a user, encrypted content data to be received related to the promotional offering metadata~~;

executing an emulator to enable a single player application of the encrypted content data to receive content data over the broadcast channel as if the single player application is receiving the encrypted content data from a telecommunication infrastructure, thereby enabling the single player application to perform the following steps regardless from where the encrypted content has been received:

~~retrieving the encrypted content data from a user's system via a second channel, the encrypted content data selected from the promotional metadata, and wherein the encrypted content data has been previously encrypted using a first encrypting key, wherein the first encrypting key is a symmetric key with a corresponding first decrypting key, wherein the second channel is selected from the group consisting of a telecommunications network, a broadcast transmission, and a computer removable storage medium;~~

~~receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the encrypted content data~~

~~received via the second web broadcast channel, wherein the first decrypting key has been encrypted with a second encrypting key of a trusted third party;~~

transferring to a trusted third party an~~the~~ encrypted first decrypting key, which has been encrypted with a~~the~~ second encrypting key of the trusted third party~~, to the trusted third party~~;

receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key; and

decrypting, ~~on the user's system~~ in a tamper resistant environment of the single player application, the encrypted first decrypting key with the user's system key.

8. (Currently Amended) The method as defined in claim 7, ~~wherein the step of assembling at least part of the promotional data includes assembling at least part of the promotional data into a format readable by a web browser and wherein the step of selecting includes selecting with a web browser~~ further comprising receiving the encrypted first decrypting key over a computer readable medium which is different than the web broadcast channel.

9. (Currently Amended) The method as defined in claim 7, wherein the step of ~~selecting~~receiving includes ~~selecting promotional material that has been previously received and stored~~storing on the user's system the encrypted content data for later decrypting by the player application.

10. (Currently Amended) The method as defined in claim 9, wherein the step of ~~selecting~~receiving the encrypted content data further comprises the sub-steps of:

determining a schedule for next ~~web~~ broadcast of the encrypted content data selected;

setting a trigger to trigger the user's system to receive the next ~~web~~ broadcast ~~on the second channel~~ of the encrypted content data selected.

11. (Currently Amended) The method as defined in claim 10, further comprising:

receiving promotional metadata related to the encrypted content data over the broadcast channel;

selecting by a user, encrypted content data to be received related to the promotional offering metadata;

wherein the step of ~~retrieving~~receiving encrypted content data includes receiving encrypted content data from a second broadcast channel~~, includes receiving the encrypted content data~~ selected from the promotional metadata on ~~a web~~the second broadcast channel and a time provided by the trigger.

12. (Currently Amended) The method as defined in claim ~~7~~11, wherein the step of ~~etrieving~~receiving encrypted content data from a second channel includes receiving data in a format compatible with DirecPC™.

13. (Currently Amended) The method as defined claim ~~7~~11, wherein the step of receiving data from a second channel includes the sub-step of:

authorizing over a back channel that the user's system is authorized to receive the encrypted content data selected; and wherein the step of receiving the encrypted first decrypting key includes receiving the encrypted first decrypting key only if the user's system is authorized by the trusted third party to receive the encrypted content data selected.

14. (Currently Amended) The method as defined claim ~~7~~11, wherein the step of receiving encrypted content data from a second channel further includes the sub-step of:

~~Notifying~~presenting to the user, the next time the user starts the user's system, a status if the current encrypted content data selected from the promotional metadata has been received on the user's system.

15. (Previously Presented) The method as defined in claim 7, wherein the step of receiving the encrypted content data, includes receiving the encrypted content data along with a network address of the trusted third party.

16. (Currently Amended) The method as defined in claim ~~15, wherein the step of~~ 7 further comprising receiving the encrypted first decrypting key ~~includes receiving the first decrypting key~~ over a broadcast stream.

17. (Currently Amended) The method defined in claim ~~15~~ 7, wherein the ~~network address of the trusted third party is an address of a clearinghouse~~ tamper resistant environment forms reencrypted content data by reencrypting the content data with a locally generated ~~digital content~~ player application encrypting key, wherein the locally generated player application key requires less processing utilization than the first decrypting key to provide real-time decryption of the content data.

18. (Currently Amended) The method defined in claim 15, wherein the first decrypting key has a timeout provision for decrypting the content data.

Claims 19 - 20. (Withdrawn)

21. (Currently Amended) A user's system for securely receiving data from a web broadcast infrastructure with a plurality of channels, comprising:

a receiver for receiving promotional metadata from a ~~first web~~ broadcast channel, the promotional metadata related to data available for reception;

~~an interface to an output device for presenting at least part of the promotional metadata for review by a user;~~

~~an interface to an input device for receiving a selection by a user of the data to be received related to the promotional metadata;~~

a controller for controlling the receiver to receive encrypted content data from the~~a second web~~ broadcast channel, the encrypted content data selected from the promotional metadata, and wherein the encrypted content data has been previously encrypted using a first encrypting key~~, wherein the first encrypting key is a symmetric key with~~having a corresponding first decrypting key~~;, wherein the second channel is selected from the group consisting of a telecommunications network, a broadcast transmission, and a computer removable storage medium; and~~

~~an interface for receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel~~, wherein the first decrypting key has been encrypted with a second encrypting key of a trusted third party;

a single player application for rendering the encrypted content data;

an emulator to enable the single player application of the encrypted content data to receive content data over the broadcast channel as if the single player application is receiving the encrypted content data from a telecommunication infrastructure, thereby enabling the single player application to perform the following steps regardless from where the encrypted content has been received:

transferring to the trusted third party the encrypted first decrypting key, which has been encrypted with the second encrypting key~~ to the trusted third party~~;

receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key; and

decrypting, in a tamper resistant environment of the single player application, the encrypted first decrypting key with the user's system key.

decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with the user's system key;

wherein the tamper resistant environment forms reencrypted content data by reencrypting the content data with a locally generated ~~digital content~~ player application encrypting key, wherein the locally generated player application key requires less

processing utilization than the first decrypting key to provide real-time decryption of the content data.

22. (Currently Amended) The user's system as defined in claim 21, wherein the ~~output device is a web browser and the input device is coupled to the web browser for receiving a selection by a user~~ the encrypted content data, includes a network address of the trusted third party.

23. (Currently Amended) The user's system as defined in claim 21, wherein the controller further comprises:

a schedule derived from the promotional metadata wherein the schedule is used to control the receiver to receive encrypted content data from ~~a second web~~ the broadcast channel.

24. (Currently Amended) The user's system as defined in claim 21, wherein the receiver is adapted to receive encrypted content data broadcasted in a format compatible with DirecPC™.

Claim 25 (Withdrawn)